# Tips on using anti-virus software effectively

The beginner section gave a run through of useful anti-virus software such as [Avast](https://www.avast.com) or [Clam Win](http://www.clamwin.com/) and anti-malware software such as [Spybot](https://www.safer-networking.org/) or [Malwarebytes](https://www.malwarebytes.org/). There are a few ways in which you can make sure you get the most out of your software.

* Do not run two anti-virus programs at the same time, as this might cause your computer to run extremely slowly or to crash. Uninstall one before installing another. However anti-malware software is designed to work alongside anti-virus software.
* Make sure that your anti-virus program updates itself regularly. Without updates it can quickly become ineffective. All of the software recommended here supports free updating.
* Enable your anti-virus software's 'always on' virus-detection feature if it has one. It may also be called 'Realtime Protection,' 'Resident Protection,' or something similar.
* Scan all of the files on your computer regularly. You don't have to do this every day but you should do it from time to time. How often may depend on the circumstances. Have you connected your computer to unknown networks recently? With whom have you been sharing USB memory sticks? Do you frequently receive strange attachments by email? Has someone else in your home or office recently had virus problems? Tools such as Avast can do this for you.

# Preventing virus or spyware infection

* If you need to open a file from someone you don?t know well, you should save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the program's File menu to open the attachment manually, rather than double-clicking the file or allowing your email program to open it automatically, you are less likely to contract a virus.
* Hover over URLs and hyperlinks to check where they lead. If you're unsure about a URL, check it at [VirusTotal](https://www.virustotal.com/#url).
* Before inserting removable media, such as CDs or USB sticks, into your computer, you should disable your operating system's 'AutoPlay' feature. (This is usually found under the Properties section of My Computer)
* Improve the security of your Web browser by preventing it from automatically running the potentially dangerous programs that are sometimes contained within webpages you visit. If you are using Mozilla Firefox, you can install the NoScript add-on.
* Download over an encrypted connection (usually SSL in the browser) whenever possible.
* Using free and open-source software significantly lowers your risk of being infected by malware. These tools are often written and updated for free by volunteers and are generally more secure than their proprietary alternatives. In particular, you should consider replacing Internet Explorer, Outlook and Microsoft Office with Firefox, Thunderbird and LibreOffice, respectively. You should also consider switching from the Microsoft Windows operating system to a more secure open-source alternative like Ubuntu or ChromeOS.

# Preventing untrusted network connections

* A firewall helps to protect your computer from unauthorised connections to and from the Internet. It can also help reduce the spread of malware if you are infected. Most operating systems have firewalls included but check to make sure they are turned on. (You can usually find this under Control Panel > Security) There are also excellent free programs such as [Comodo](https://securityinabox.org/comodofirewall_main) Personal Firewall, which can help keep your computer secure.
* Make sure that all of the computers on your office network have a firewall installed. Read more about this in the Network Section.
* Only install essential programs on the computer you use for sensitive work, and make sure you get them from a reputable source. Uninstall any software that you do not use.

Swipe right for this lesson's checklist

Go to the Beginner lesson for basic advice on how to identify and protect yourself against malware.

[Go to Beginner Lesson](umbrella://lesson/malware/0)